(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Numéro de publication : **0 632 413 A1**

(12) DEMANDE DE BREVET EUROPEEN

(21) Numéro de dépôt : **94401499.2**

(22) Date de dépôt : **01.07.94**

(51) Int. Cl.[6] : **G07C 9/00**, G07F 7/10

(30) Priorité : **01.07.93 FR 9308073**

(43) Date de publication de la demande :
04.01.95 Bulletin 95/01

(84) Etats contractants désignés :
AT BE CH DE DK ES FR GB GR IT LI LU NL SE

(71) Demandeur : **BULL CP8**
68 route de Versailles,
B.P. 45
F-78430 Louveciennes (FR)

(72) Inventeur : **Patarin, Jacques**
11, rue Amédée Dailly
F-78220 Viroflay (FR)
Inventeur : **Ugon, Michel**
6, rue des Cépages
F-78310 Maurepas (FR)

(74) Mandataire : **Corlu, Bernard Edouard et al**
Bull S.A.,
68, route de Versailles,
B.P. 45,
PC/LV-59C18
F-78430 Louveciennes (FR)

(54) Procédé de saisie d'une information confidentielle et terminal associé.

(57) L'information confidentielle étant composée de signes appartenant à une première série (3), on définit une seconde série de signes (4), on affiche la première et la seconde séries de signes selon une position relative aléatoire, et on utilise cette mise en correspondance pour saisir l'information confidentielle de sorte qu'un tiers qui observe les opérations de saisie ne peut pas déterminer l'information confidentielle.

L'invention concerne aussi le terminal associé à ce procédé.

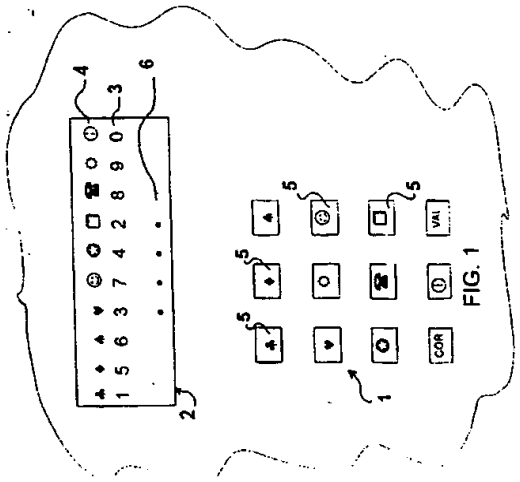

FIG. 1

EP 0 632 413 A1

La présente invention concerne un procédé de saisie, par un terminal, d'une information confidentielle fournie par un utilisateur, cette information comprenant plusieurs signes appartenant à une première série de signes.

Il est connu que les moyens de paiement électroniques utilisant une carte associée à un terminal se généralisent, qu'il s'agisse de distributeurs de billets ou de moyens de paiement dans les magasins.

Pour identifier le porteur d'une carte ou un opérateur, il est souvent demandé à ce dernier d'introduire une information confidentielle, couramment appelée code, au moyen d'un clavier associé au terminal. Les conditions dans lesquelles le code doit être introduit au moyen du clavier ne permettent généralement pas de masquer le clavier de façon satisfaisante de sorte que celui-ci peut être observé par un tiers pendant la saisie de l'information confidentielle. Une personne mal intentionnée peut donc ensuite utiliser cette information à des fins frauduleuses.

Certains systèmes comportent des claviers dont les signes sont disposés selon des positions qui varient d'un clavier à un autre de sorte que pour un tiers qui ne connaît pas la disposition des signes sur un clavier en cours d'utilisation, il n'est pas possible de deviner l'information confidentielle en observant simplement la position des touches qui sont frappées par l'utilisateur. Ceci a toutefois pour inconvénient de compliquer sensiblement la réalisation du clavier et engendre des erreurs d'introduction de l'information confidentielle lorsque des utilisateurs, habitués à une certaine disposition des signes, ne prêtent pas attention au fait que le clavier considéré ne comporte pas la disposition habituelle. En outre, un fraudeur expérimenté peut analyser la répartition des signes sur un clavier précis avant ou après la saisie de l'information confidentielle par l'utilisateur et mémoriser la position des touches frappées pour en déduire finalement l'information confidentielle.

Un but de la présente invention est de proposer un procédé de protection d'une information confidentielle comprenant plusieurs signes appartenant à une première série de signes lors de l'opération de saisie de cette information même lorsque cette opération peut être observée par un tiers.

En vue de la réalisation de ce but, le procédé selon l'invention consiste à définir une seconde série de signes; à afficher, sur des moyens d'affichage, les première et seconde séries de signes de façon que chaque signe de la première soit disposé en regard d'un signe de la seconde, et à utiliser des signes de la seconde série de signes en regard desquels se trouvent les signes de la première série de signes composant ladite information confidentielle pour la désignation par l'utilisateur de cette information confidentielle.

Ainsi, l'utilisateur ne désigne pas directement les signes composant l'information confidentielle mais des signes - ceux de la seconde série - qui sont corrélés à ceux-ci selon un lieu de corrélation qui n'apparaît pas explicitement sur les moyens d'affichage. En conséquence, la seule observation des moyens d'affichage par un tiers ne permet pas à celui-ci d'en déduire les signes confidentiels saisis.

Selon une première variante du procédé selon l'invention, on utilise un clavier distinct des moyens d'affichage et comportant plusieurs touches, on identifie chacune des touches du clavier en lui affectant un signe appartenant à la seconde série de signes, on affiche, sur des moyens d'affichage, les première et seconde séries de signes selon une distribution mutuelle aléatoire connue du terminal; et on réalise la désignation des signes de la première série composant ladite information confidentielle en actionnant chaque touche du clavier dont le signe correspond au signe de la seconde série situé en regard de l'un des signes, appartenant à la première série, constituant de ladite information confidentielle.

Ainsi, lorsqu'un utilisateur saisit une information confidentielle, les touches du clavier qu'il frappe ne comportent pas les signes de son code mais des signes correspondants selon une correspondance qui est donnée à l'utilisateur par l'affichage simultané des deux séries de signes. Etant donné que cette correspondance varie pour chaque saisie de l'information confidentielle en fonction du positionnement relatif des séries de signes, la seule connaissance des touches frappées sur le clavier lors d'une saisie est sans utilité pour un fraudeur.

Selon une version avantageuse de cet aspect de l'invention, au moins l'une des séries de signes disparaît dès qu'une touche est frappée. Ainsi, il n'est pas possible pour un fraudeur de regarder d'abord la touche qui est frappée puis de prendre connaissance du signe correspondant de la première série en observant les séries affichées.

A l'aide des versions précédemment décrites, l'utilisateur peut désormais saisir une information confidentielle sans divulguer le moindre renseignement à un tiers n'observant que le clavier ou que l'écran.

Selon une seconde variante du procédé selon l'invention, une solution au problème d'un tiers observant à la fois l'écran et le clavier est apportée; pour ce faire, on définit secrètement, parmi les signes de la seconde série, au moins un signe de référence connu du terminal et de l'utilisateur, puis on fait afficher, en regard des signes de la seconde série de signes, des signes de la première série de façon qu'à chaque fois, l'un des signes composant ladite information confidentielle soit disposé en regard dudit signe de référence.

Selon une version avantageuse de cet aspect de l'invention, on affiche l'ensemble des signes de la première série dans un ordre quelconque pendant toute l'opération de saisie, on provoque le décalage

de cet ensemble par rapport à celui des signes de la seconde série afin de disposer au moins un signe composant ladite information confidentielle devant ledit signe de référence et on valide la saisie lorsque l'utilisateur envoie un ordre de validation au terminal indiquant qu'il a placé ce signe confidentiel en regard du signe de référence.

Selon encore une autre version de l'invention dans lequel le terminal comprend un clavier à plusieurs touches, on identifie chacune des touches dudit clavier en lui affectant un signe appartenant à la première série de signes et on affiche, pour chaque touche actionnée, le signe de la première série affecté à cette touche en regard d'un signe de la seconde série, le terminal étant agencé pour effectuer une comparaison entre le signe de la première série ainsi placé par l'utilisateur devant le signe de référence et au moins un des signes de l'information confidentielle.

L'invention concerne aussi un terminal comprenant des moyens d'affichage et des moyens pour saisir une information confidentielle fournie par un utilisateur, ladite information comprenant plusieurs signes appartenant à une première série de signes, ledit terminal étant agencé pour afficher, sur des moyens d'affichage, ladite première et une seconde séries de signes de façon que chaque signe de la première série soit disposé en regard d'un signe de la seconde série et comportant, d'une part, des moyens d'utilisation des signes de la seconde série situés en regard des signes constituant l'information confidentielle pour permettre à l'utilisateur de désigner les signes de la première série qui composent ladite information confidentielle et d'autre part, des moyens de validation des saisies.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description qui suit de différentes versions de l'invention en relation avec les figures ci-jointes parmi lesquelles :

- la figure 1 illustre de façon schématique une partie d'un terminal mettant en oeuvre une première variante du procédé selon l'invention,
- la figure 2 est une représentation schématique de l'écran d'affichage dans une étape postérieure à la figure 1, en relation avec une variante de réalisation du procédé selon l'invention,
- la figure 3 est une illustration schématique de l'écran d'un terminal en relation avec une autre version du procédé selon l'invention,
- la figure 4 est une illustration de l'écran du terminal postérieurement à la figure 3, en relation avec la version du procédé de la figure 3.
- la figure 5 est une autre illustration du procédé selon la figure 3, comportant une seconde série de signes constituée de flèches, et
- la figure 6 illustre de façon schématique une partie d'un terminal mettant en oeuvre une seconde variante du procédé selon l'invention.

En référence à la figure 1, une première variante de réalisation du procédé selon l'invention est destinée à permettre la protection d'une information confidentielle, par exemple le code d'une carte bancaire, lors de sa saisie sur un clavier d'un terminal. Sur la figure 1 on a représenté seulement le clavier du terminal généralement désigné en 1, et l'écran d'affichage du terminal généralement désigné en 2. De façon connue en soi, l'information confidentielle est composée de signes appartenant à une série de signes, par exemple des chiffres dans l'exemple illustré. Dans la suite de la description, on supposera que l'information confidentielle est composée de quatre signes et que dans les exemples illustrés, ces quatre signes sont les chiffres 4723.

Selon cette variante de l'invention, on représente sur les touches 5 du clavier 1 du terminal, une seconde série de signes et on affiche sur le terminal d'une part la première série de signes qui est ici disposée selon une ligne 3 sur l'écran d'affichage, et d'autre part la seconde série de signes qui est ici disposée selon une ligne 4 sur l'écran d'affichage au-dessus de la ligne 3 de la première série de signes, la première et la seconde séries de signes étant affichées selon une position relative aléatoire c'est-à-dire que la correspondance entre les signes de la première série et les signes de la seconde série peut varier chaque fois qu'une carte est introduite dans le terminal. Ainsi, les touches qui doivent être frappées sur le clavier varient à chaque nouvel affichage des deux séries de signes de sorte qu'un tiers qui observe seulement les touches frappées par l'utilisateur ne pourra pas réutiliser l'information obtenue lors d'une saisie ultérieure.

Selon une première version de l'invention, on suppose que la première et la seconde série de signes restent affichées avec la même position relative pendant que l'utilisateur saisit les différents signes sur le clavier. Dans le cas envisagé, l'utilisateur va donc frapper successivement sur le clavier les touches comportant 9 puis ☺, puis π, et enfin ♥. Pour faciliter la saisie de l'information confidentielle par l'utilisateur, l'écran d'affichage 2 comporte de préférence de façon habituelle une ligne 6 de repères indiquant le nombre de signes déjà saisis et permettant ainsi à l'utilisateur de savoir à quelle position de l'information confidentielle il se trouve. Dans l'exemple illustré les signes de la ligne 6 sont au départ des points qui sont progressivement remplacés par des étoiles chaque fois que l'utilisateur saisit un signe.

On remarquera que dans cette version du procédé de l'invention un fraudeur qui observe seulement le clavier ne peut en aucune façon appréhender l'information confidentielle puisqu'il ne connaît pas la correspondance entre les signes frappés sur le clavier et les chiffres qui composent le code. Toutefois, s'il a en plus la possibilité de voir l'écran, il pourra mé-

moriser la correspondance entre les deux séries de signes, ou plus simplement regarder cette correspondance chaque fois qu'il verra l'utilisateur frapper une des touches du clavier. En effet, la lecture de la correspondance implique une tension relativement soutenue de l'utilisateur qui a tendance à vérifier qu'il ne se trompe pas de signes de la seconde série et agit donc plus lentement que d'habitude. Dans ce cas, il sera donc possible pour un fraudeur qui aura vu l'utilisateur frapper la touche 9 de regarder ensuite l'écran et de constater que 9 correspond au chiffre 4, et d'effectuer ainsi successivement le décodage des signes frappés par l'utilisateur.

Pour éviter une telle manoeuvre du fraudeur, on prévoit de préférence, selon une autre version de l'invention, de changer la position relative de la première et de la seconde série de signes après la saisie de chaque signe de l'information confidentielle. Ainsi, même lorsqu'un tiers a la possibilité d'observer non seulement le clavier mais également l'affichage des séries de signes, la fréquence de changement très importante de la correspondance entre les signes de la première série et de la seconde série augmente la difficulté de mémoriser cette correspondance simultanément à la position de la touche frappée par l'utilisateur. On a illustré sur la figure 2 l'affichage qui est vu par l'utilisateur sur l'écran dès qu'il a frappé la touche 9. Selon la version illustrée, la seconde série de signes est restée dans la même position mais la première série de signes est affichée selon une nouvelle disposition des chiffres tandis que dans la ligne de repères 6 le premier point a été remplacé par une étoile. Selon cette version de l'invention, après avoir commencé comme précédemment par frapper la touche 9, l'utilisateur va donc cette fois frapper la touche ♠ qui correspond au deuxième chiffre, 7, de son code. On remarquera qu'il n'est donc pas possible pour un fraudeur qui a attendu de voir la touche frappée par l'utilisateur de déterminer le signe correspondant de la première série. En effet, le fraudeur qui a attendu de voir l'utilisateur frapper la touche 9 et qui regarde alors l'écran d'affichage lira que le chiffre correspondant à 9 est le chiffre 3 et fera donc une erreur dans l'appréciation du premier chiffre de l'information confidentielle. Pour pouvoir obtenir l'information confidentielle, le fraudeur devra donc mémoriser successivement les correspondances entre la première et la seconde série de signes avant que l'utilisateur ne frappe un signe, ce qui réduit considérablement le risque d'avoir un fraudeur capable de mémoriser l'ensemble des signes de l'information confidentielle.

Dans l'exemple illustré sur les figures 1 et 2, les deux séries de signes sont affichées sur l'écran mais seuls les signes de la première série ont une position variable. On remarquera qu'il est bien entendu possible de faire varier également la position des signes de la seconde série ou encore de faire varier la position des signes de la seconde série tout en maintenant fixe la position des signes de la première série.

Les figures 3 à 5 illustrent une autre version du procédé selon l'invention. Dans cette version, les signes de la seconde série sont cette fois disposés en dessous des signes de la première série et sont disposés de façon fixe sur le boîtier du terminal en dessous de l'écran d'affichage. Cette disposition ne caractérise pas cette version du procédé de l'invention et l'on pourrait adopter pour les signes la même disposition que sur les figures 1 et 2. Ce qui caractérise cette version du procédé de l'invention est le fait que la seconde série de signes comporte cette fois un nombre de signes distincts inférieur à la première série de signes de sorte que pour avoir une correspondance entre chacun des signes de la première série de signes et les signes de la seconde série de signes, il est nécessaire d'affecter un même signe de la seconde série à plusieurs signes de la première série. Dans l'exemple illustré sur les figures 3 et 4, la première série de signes comporte comme précédemment dix chiffres, de zéro à neuf, et la seconde série de signes comporte cette fois cinq signes distincts seulement qui sont ☺, 9, ☼, ♥, ☎. Afin qu'un signe de la seconde série corresponde à chaque signe de la première série, certains signes de la seconde série sont représentés avec une accolade pour montrer les signes de la première série auxquels ils sont affectés. Ainsi le ☺ est affecté à deux chiffres ainsi que le 9 et le ♥ tandis que le ☼ est affecté à trois chiffres et le ☎ est affecté à un seul chiffre.

Lors de l'introduction d'une carte, les signes de la première série sont affichés de façon aléatoire pour qu'à chaque signe de la première série corresponde un signe de la seconde série. On remarquera à ce propos que la position des signes de la première série peut être totalement aléatoire, c'est-à-dire que les signes de la première série sont disposés non seulement de façon aléatoire par rapport aux signes de la seconde série, mais sont également disposés de façon aléatoire les uns par rapport aux autres, ou de façon pseudo-aléatoire c'est-à-dire que tout en étant disposés de façon aléatoire par rapport aux signes de la seconde série, les chiffres de la première série sont disposés de façon ordonnancée les uns par rapport aux autres. C'est le cas dans l'exemple illustré sur la figure 3 où les chiffres sont ordonnés les uns par rapport aux autres selon une séquence en boucle, la position aléatoire par rapport aux signes de la seconde série étant déterminée par un décalage aléatoire de la séquence. En particulier sur la figure 3, le zéro correspond à la deuxième case du ☼ de la seconde série.

En supposant que la position des signes de la première série reste constante pendant toute la saisie de l'information confidentielle, un utilisateur ayant le

code 4723 va donc saisir, dans le cas de la figure 3, successivement les signes 9, ☼, ♥ et ☺. Contrairement à la version qui avait été décrite en relation avec la figure 1, un fraudeur qui observera simultanément le clavier et l'écran ne pourra pas en déduire avec certitude l'information confidentielle saisie par l'utilisateur. En effet, lorsqu'un fraudeur voit l'utilisateur saisir le premier signe 9, il ne peut savoir si ce signe correspond au chiffre 1 ou au chiffre 4. De même, lorsque l'utilisateur saisit le signe ☼, un observateur ne peut savoir si ce ☼ correspond au chiffre 0, au chiffre 5 ou au chiffre 7. De même, le signe ♥ correspond au chiffre 2 ou au chiffre 8. Seul le signe ☎ correspond uniquement au chiffre 6. Dans ce cas la même séquence de signes de la seconde série aurait été saisie par un utilisateur dont le code aurait été 1529 ou 4089.

En supposant qu'un observateur ait réussi à mémoriser la correspondance complète entre les signes de la première et de la seconde série, et la succession des touches frappées par l'utilisateur et qu'il veuille réutiliser cette information lors d'une saisie ultérieure, il se trouvera confronté à une nouvelle table de correspondance comme illustré par exemple sur la figure 4. Sur cette figure, un nouveau décalage a été effectué entre la série de chiffres formant la première série de signes et la seconde série de signes. Il se trouve que le choix entre le 1 et le 4 qui a pu être relevé par un observateur lors de la saisie précédente, se trouve cette fois illustré par un ☺ et un ☎, c'est-à-dire qu'il existe une chance sur deux pour le fraudeur de se tromper dans la saisie du premier signe constituant l'information confidentielle. De même, un fraudeur aura de nouveau un doute concernant le second signe à saisir puisque les chiffres 0, 5 et 7 qui correspondaient au signe ☼ dans la figure 3 sont représentés sur la figure 4 par les signes ♥, ○ ou ☺. On remarque donc que la probabilité pour un observateur de pouvoir ressaisir exactement l'information confidentielle est extrêmement faible. Ce risque est encore minimisé si l'on prévoit comme précédemment de changer la correspondance entre la première série de signes et la seconde série de signe chaque fois qu'un signe vient d'être saisi.

La variante de la figure 5 se distingue de celle de la figure 3 en ce que les pictogrammes élaborés, constitués par les signes de la seconde série, sont remplacés ici par des signes plus simples, construits à partir d'un seul signe élémentaire, à savoir un triangle isocèle. La seconde série de signes comprend cinq signes, chacun se distinguant par un nombre de triangles particuliers ou une orientation particulière de ceux-ci. Ainsi, les chiffres 2 à 4 de la première série de signes sont tous les trois désignés par le même signe constitué par deux triangles 6 juxtaposés et orientés vers la droite de la figure 5. Une accolade 7 définit cette correspondance. Les chiffres 0 et 1 sont désignés par un seul triangle 6 ayant la même orientation que pour les chiffres 2 à 4. Une seconde série de ce type, construite à partir d'un seul signe simple, est avantageuse en ce que l'utilisation mémorise immédiatement l'ensemble des signes utilisés. Par ailleurs, les chiffres de la première série de signes (par exemple 2 à 4) désignés par le même signe de la seconde série sont juxtaposés, de sorte qu'un seul signe (ici, les deux triangles 6) les désignent simultanément, ce qui facilite encore la tâche de l'utilisateur.

La figure 6 illustre une autre variante de réalisation du procédé dans laquelle on a supposé que, en plus des chiffres 4723, le code confidentiel de l'utilisateur comprend deux signes de référence secrets 3 et 9 parmi les signes de la seconde série, tous ces signes étant connus de l'utilisateur et du terminal lors de la saisie. Ces signes de référence peuvent être par exemple fournis à l'utilisateur, en même que l'information confidentielle, par l'organisme habilité, lors de la souscription au service demandé.

Dans cette figure 6 les deux séries sont identiques, les signes les composant étant ici les chiffres de 0 à 9. Le terminal affiche donc la seconde série de signes 61, soit de façon figée, les signes étant gravés sur les moyens d'affichages, soit de façon aléatoire. Des cases d'affichages sont prévues afin d'afficher en regard de ces signes de la seconde série ceux de la première qui vont être saisis. Dans l'exemple de la figure 6, on a grisé les cases 63 correspondant aux cases placées en regard des signes de référence 3 et 9. Bien entendu, l'affichage à l'écran étant banalisé, il n'apparaît aucune indication permettant à un fraudeur de déterminer lesquels des signes affichés sont ceux de référence.

Le clavier 65 associé à ces moyens d'affichage comporte des touches identifiées par les signes 0 à 9 et permet à l'utilisateur d'entrer ces signes qui sont alors affichés au fur et à mesure des saisies dans les cases situées en regard des signes de la seconde série. L'utilisateur va donc entrer des signes sans intérêt dans toutes les cases autres que celles ici référencées 63. Au contraire, il entre les deux premiers chiffres, 4 et 7, de son information confidentielle dans ces cases 63. Cette saisie est complète lorsque toutes les cases sont remplies et le terminal propose alors à l'utilisateur d'entrer de nouveau une série de signes en regard de la série comportant les signes de référence, afin de saisir de la même façon les deux chiffres de son information confidentielle 2 et 3 restants. Pour un observateur tiers, il est possible au prix d'un effort de mémorisation supplémentaire de retenir la combinaison totale saisie, mais il n'a aucun moyen de déterminer lesquels des signes ont une importance particulière. Dans le cas où les signes de la seconde série sont affichés au départ de façon aléatoire, saisir cette combinaison ne lui apporte rien.

On peut aussi prévoir un système de défilement de signes de la première série sous forme d'une séquence affichée en regard de la seconde série. Des moyens de décalage de ces signes sont prévus à cet effet. Par exemple, deux touches de décalage, respectivement vers la gauche et vers la droite, ou bien même une seule touche provoquant le défilement cyclique des signes de la première série, peuvent être utilisées.

A chaque pression sur une de ces touches, ou après un laps de temps donné assez court, la séquence est donc décalée d'une position dans le sens choisi, et ce de façon cyclique, afin qu'il y ait toujours un signe de la première série placé en regard d'un signe de la seconde. Lorsque le premier signe de l'information confidentielle se situe en regard d'un des signes de référence, l'utilisateur donne un ordre de validation, par exemple à l'aide d'une touche de validation ou par une commande vocale.

Les signes d'au moins une des deux séries sont alors affichés selon une nouvelle séquence aléatoire avant l'entrée du signe suivant de l'information confidentielle. Cela suffit en général à indiquer à l'utilisateur que le signe précédent a été effectivement saisi par le système et que le système attend la saisie suivante.

Le cycle se répète jusqu'à ce que la totalité de l'information confidentielle soit saisie. A la fin de l'opération, on peut simplement faire afficher un message ou effacer les séquences de signes, signalant à l'utilisateur que la saisie est terminée. On peut aussi prévoir l'affichage d'un caractère, par exemple un signe *, pour chaque signe saisi.

Dans le cas présenté à la figure 6, les signes de l'information confidentielle sont entrés de façon ordonnée, suivant un arrangement (1..i..n). Afin de confondre un observateur, cette information peut être saisie de façon désordonnée. Le terminal présente à cette fin un message demandant à l'utilisateur de placer son ou ses signes de rang i regard de son ou ses signes de référence. De cette façon, l'ordre de saisie est brouillé et change à chaque nouvelle saisie.

Dans le cas où l'information confidentielle est composée de chiffres, comme dans l'exemple de la figure 6, le message du terminal peut de plus demander à l'utilisateur de placer le chiffre résultant d'une fonction de ceux de rang i, j de son information confidentielle en regard des signes de référence. Bien entendu, cette fonction est modifiée lors de chaque saisie.

Supposons maintenant que le message comporte :

Case secrète 1 : mettez votre chiffre de code de rang 3, plus 1

Case secrète 2 : mettez votre chiffre de code de rang 1, moins 1.

L'utilisateur doit alors saisir les chiffres 3 (chiffre 2 plus 1) et 3 (chiffre 4 moins 1) dans les cases 63 correspondant aux signes de référence. Un fraudeur éventuel qui prend connaissance du message et qui retient les chiffres saisis ne sait pas auxquels des chiffres saisis il doit appliquer ces fonctions pour obtenir l'information confidentielle.

Bien entendu l'invention n'est pas limitée au mode de réalisation décrit et on peut y apporter des variantes de réalisation sans sortir du cadre de l'invention. En particulier, bien que les signes de la première série aient été illustrés par des chiffres, on peut prévoir des signes quelconques, les signes utilisés pouvant même être différents d'une carte à une autre, l'affichage des signes de la première série étant alors fait par le terminal en fonction d'une codification contenue dans la carte.

On peut également prévoir des signes identiques pour la première et la seconde séries de signes. Il faut dans ce cas que les séries de signes soient clairement indiquées sur l'écran d'affichage sans quoi le risque d'erreurs de saisie risque d'être très grand.

Revendications

1. Procédé de saisie, par un terminal, d'une information confidentielle fournie par un utilisateur, cette information comprenant plusieurs signes appartenant à une première série de signes (3), caractérisé en ce qu'il comprend les étapes suivantes consistant à :
   - définir une seconde série de signes (4);
   - afficher, sur des moyens d'affichage, les première et seconde séries de signes de telle façon que chaque signe de la première série de signes soit disposé en regard d'un signe de la seconde série de signes; et
   - utiliser des signes de la seconde série de signes en regard desquels se trouvent les signes de la première série de signes composant ladite information confidentielle pour la désignation par l'utilisateur de cette information confidentielle.

2. Procédé selon la revendication 1, caractérisé en ce que l'on utilise un clavier (1) distinct des moyens d'affichage et comprenant plusieurs touches, et en ce que l'on procède aux étapes suivantes consistant à :
   - identifier chacune des touches du clavier en lui affectant un signe appartenant à la seconde série de signes (4);
   - afficher, sur les moyens d'affichage, les première et seconde séries de signes selon une distribution mutuelle aléatoire, connue du terminal; et
   - la désignation des signes de la première série composant ladite information confidentielle se fait en actionnant chaque touche du

clavier (1) dont le signe correspond au signe de la seconde série (4) situé en regard de l'un des signes de la première série (3) constituant ladite information confidentielle.

3. Procédé selon la revendication 2, caractérisé en ce qu'au moins l'une des séries de signes (3, 4) disparaît dès qu'une touche du clavier (1) est frappée.

4. Procédé selon la revendication 1, caractérisé en ce qu'il comprend les étapes suivantes :
   - définir secrètement, parmi les signes de la seconde série (4), au moins un signe de référence connu du terminal et de l'utilisateur; et
   - afficher, en regard des signes de la seconde série de signes, respectivement, les signes de la première série de telle façon qu'à chaque fois l'un des signes confidentiels composant ladite information confidentielle soit disposé en regard dudit signe de référence.

5. Procédé selon la revendication 4, caractérisé en ce que :
   - pendant toute l'opération de saisie, l'ensemble des signes de la première série (3) est affiché dans un ordre quelconque;
   - l'ensemble de ces signes (3) est décalé par rapport à ceux de la seconde série (4) afin de disposer au moins un signe confidentiel composant ladite information confidentielle devant ledit signe de référence; et
   - l'utilisateur envoie un ordre de validation au terminal lorsque ce signe confidentiel est disposé devant le signe de référence.

6. Procédé selon la revendication 4, caractérisé en ce que l'on utilise un clavier (1) à plusieurs touches, chacune des touches étant identifiée en lui affectant un signe appartenant à la première série de signes (3), l'affichage de chacun des signes de la première série (3) en regard des signes de la seconde série (4) s'effectuant en actionnant la touche identifiée par ce signe, le terminal étant agencé pour effectuer une comparaison entre le signe de la première série ainsi placé par l'utilisateur devant le signe de référence et au moins un des signes de l'information confidentielle.

7. Procédé selon la revendication 6, caractérisé en ce l'information confidentielle comprend plusieurs signes confidentiels rangés selon un rang déterminé (1...i...n) et, avant l'affichage des signes de la première série (3) par l'utilisateur, le terminal envoie un message à celui-ci lui ordonnant de placer le signe confidentiel de rang i en regard du signe de référence.

8. Procédé selon la revendication 7, caractérisé en ce que les signes de la première série (3) composant ladite information confidentielle sont des chiffres et le terminal ordonne à l'utilisateur de placer en regard du signe de référence le résultat d'une fonction du chiffre de rang i de ladite information confidentielle.

9. Procédé selon la revendication 1, caractérisé en ce que la seconde série de signes (4) comporte un nombre de signes distincts inférieur au nombre des signes de la première série (3).

10. Procédé selon la revendication 1, caractérisé en ce que les signes de la seconde série (4) sont différents de ceux de la première série (3).

11. Terminal comprenant des moyens d'affichage et des moyens pour saisir une information confidentielle fournie par un utilisateur, ladite information comprenant plusieurs signes appartenant à une première série de signes (3), ledit terminal étant caractérisé en ce qu'il est agencé pour afficher ladite première et une seconde séries de signes (4) de telle façon que chaque signe de la première série (3) soit disposé en regard d'un signe de la seconde série (4) et il comporte :
   - des moyens d'utilisation des signes de la seconde série (4) pour permettre à l'utilisateur de désigner les signes de la première série (3) constituant ladite information confidentielle; et
   - des moyens de validation des saisies.

12. Terminal selon la revendication 11 caractérisé en ce qu'il comprend un clavier (1) distinct des moyens d'affichage et équipé de plusieurs touches (5), chacune des touches du clavier étant identifiée au moyen d'un signe appartenant à ladite seconde série de signes (4) et en ce que l'actionnement de chaque touche dudit clavier dont le signe correspond au signe de la seconde série (4) affiché en regard de l'un des signes constituant ladite information confidentielle, correspond à la saisie de ce signe constituant de ladite information confidentielle.

13. Terminal selon la revendication 11, caractérisé en ce qu'il comporte :

    des moyens de mémorisation d'au moins un signe de référence connu de l'utilisateur et appartenant à la seconde série de signes (4); et

    des moyens pour permettre à l'utilisateur de faire afficher les signes de la première série

(3) de telle façon qu'un des signes constituant l'information confidentielle soit disposé en regard dudit signe de référence.

14. Terminal selon la revendication 11, caractérisé en ce que la seconde série de signes (4) comporte un nombre de signes distincts inférieur au nombre des signes de la première série (3).

15. Terminal selon la revendication 11, caractérisé en ce que les signes de la seconde série (4) sont différents de ceux de la première série (3).

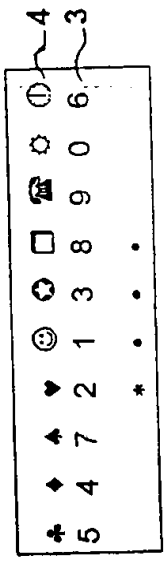

FIG. 2

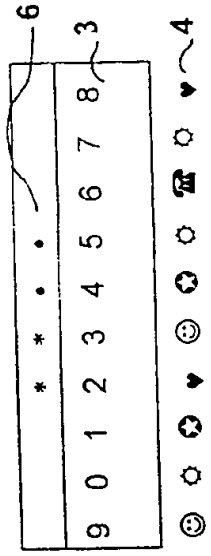

FIG. 3

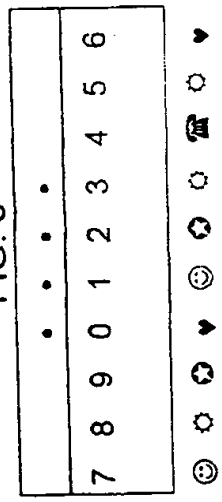

FIG. 4

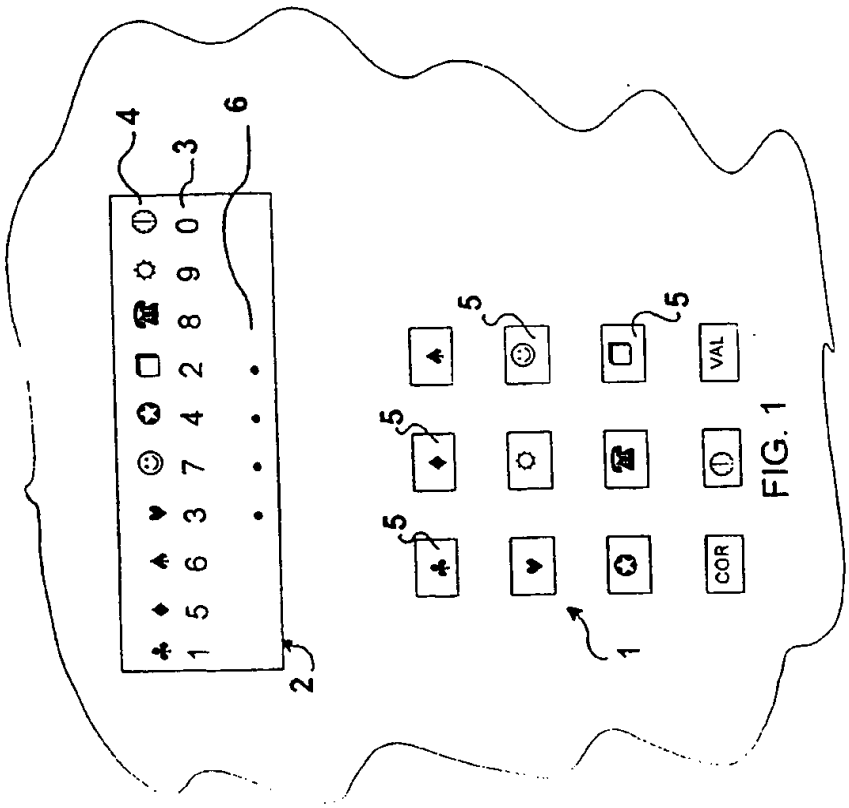

FIG. 1

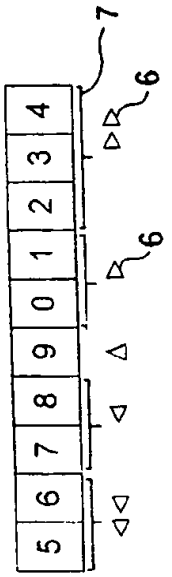

FIG. 5

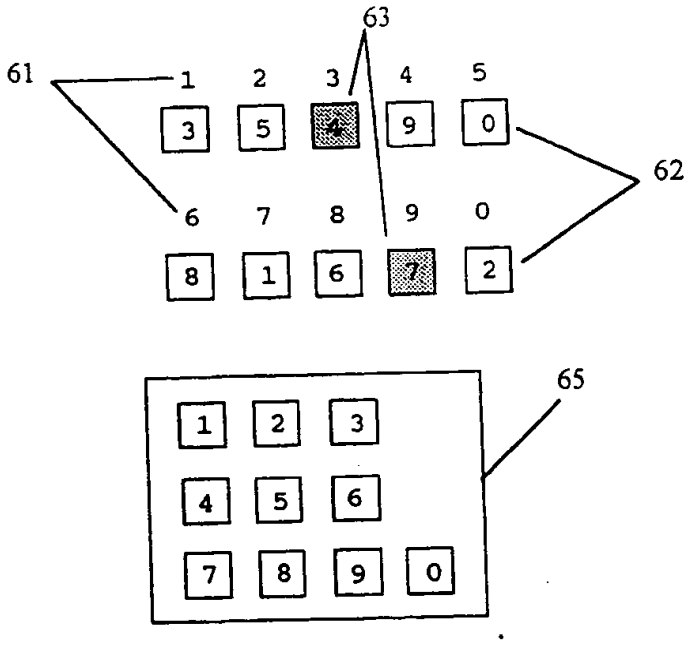

FIG. 6

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numero de la demande
EP 94 40 1499

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.6)
A	DE-A-41 29 202 (HAUNI ELEKTRONIK) * colonne 2, ligne 27 - colonne 3, ligne 32; revendications 1-5; figure 1 *	1-15	G07C9/00 G07F7/10
A	WO-A-81 02349 (REHM) * page 4, ligne 4 - page 6, ligne 13 * * page 10, ligne 24 - ligne 31; figures *	1,2,11, 12	
A	US-A-4 333 090 (HIRSCH) * abrégé; figures *	1,2,11, 12	
A	FR-A-2 459 514 (GAO) * page 1, ligne 26 - page 4, ligne 8 * * page 11, ligne 5 - page 13, ligne 30; figures *	1,11	
A	GB-A-2 153 568 (THE GENERAL ELECTRIC COMPANY) * page 1, ligne 116 - page 2, ligne 19; revendications; figures *	1,2,9, 11,12,14	
A	WO-A-93 11551 (MAURRAS) * abrégé; revendications; figures *	1,11	

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)

G07C
G07F
E05B
G06F

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
LA HAYE	14 Octobre 1994	Meyl, D

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C02)